



UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2022 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

KOLAWOLE TEMIDAYO OGUNGBESAN,
aka "Engr Jah,"
aka "Rich Jah,"
aka "Kolawole Churchill,"
aka "Bombo Klaat,"
SHOLA SOUZA, and
DEON BAKER,

Defendants.

CR 2:23-cr-00146-SVW

I N D I C T M E N T

[18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud; 18 U.S.C. § 1343: Wire Fraud; 18 U.S.C. § 1028A(a)(1): Aggravated Identity Theft; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I): Intentional Damage to a Protected Computer; 18 U.S.C. § 1956(h): Conspiracy to Engage in Money Laundering; 18 U.S.C. § 2(a), (b): Aiding and Abetting; 18 U.S.C. §§ 981(a)(1)(C), 982, 1030, and 28 U.S.C. § 2461(c): Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this Indictment:

1. A Business Email Compromise ("BEC") fraud may occur when a hacker gains unauthorized access to a victim's business email account in an attempt to trick the victim into making a unauthorized wire transfer to an account used or controlled by the hacker or others working with the hacker.

1 2. An email forwarding rule is a setting in an email system
2 that automatically forwards or redirects copies of email messages to
3 another email account.

4 3. Victim Business A, located in Irvine, California, is an
5 asset management company.

6 4. Victim Business B, located in San Francisco, California, is
7 an asset management company.

8 5. Victim Business C, located in Fort Lauderdale, Florida, is
9 a consumer experience consulting company.

10 6. Victim Business D, located in New York, New York, and
11 Chicago, Illinois, is a private equity firm.

12 7. Victim Business E, located in Bellevue, Washington, and
13 Aliso Viejo, California, is a software company.

14 8. Victim Business F, located in Phoenix, Arizona, is a
15 professional sports team.

16 9. Victim Business G, located in Boston, Massachusetts, is a
17 music technology company.

18 10. Fraudulent Business G was a fictitious business
19 incorporated in the State of Georgia under a variation of the name of
20 Victim L.P., bearing a name almost identical to Victim Business G.

21 11. Victim Business H, located in Modesto, California, is a
22 grocery company.

23 12. Fraudulent Bank Account 1 was a bank account held at Bank
24 of America with account number ending in 3344, which was held in
25 Douglasville, Georgia.

26 13. Fraudulent Bank Account 2 was a bank account held at First
27 Chatham Bank with account number ending in 6315, which was held in
28 Savannah, Georgia.

1 14. Fraudulent Bank Account 3 was a bank account held at BB&T
2 Bank with account number ending in 3375, which was held in Morrow,
3 Georgia.

4 15. Bank of America, First Chatham Bank, and BB&T Bank are each
5 federally insured.

COUNT ONE

[18 U.S.C. § 1349]

[ALL DEFENDANTS]

1. The Grand Jury re-alleges and incorporates here paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECTS OF THE CONSPIRACY

2. Beginning on an unknown date, but no later than on or about January 15, 2019, and continuing through at least April 27, 2020, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendant KOLAWOLE TEMIDAYO OGUNGBESAN, also known as ("aka") "Engr Jah," aka "Rich Jah," aka "Kolawole Churchill," aka "Bombo Klaat" ("OGUNGBESAN"), SHOLA SOUZA ("SOUZA"), and DEON BAKER ("BAKER"), together with others known and unknown to the Grand Jury, knowingly conspired to commit wire fraud, in violation of Title 18, United States Code, Section 1343, and bank fraud, in violation of Title 18, United States Code, Section 1344(2).

B. THE MANNER AND MEANS OF THE CONSPIRACY

3. The objects of the conspiracy were to be accomplished, in substance, as follows:

(a) Defendant OGUNGBESAN or his co-conspirators would identify a potential victim of BEC fraud. This would be done in part by hacking into the email system of either the potential BEC fraud victim or a party with whom the potential BEC fraud victim was communicating, and then intercepting communications and directly communicating with the potential victims.

(b) Defendant OGUNGBESAN or a co-conspirator would search a victim's email communications to identify upcoming planned wire

1 transfers.

2 (c) After gaining control of a victim's email system,
3 defendant OGUNGBESAN or a co-conspirator would often implement
4 unauthorized email forwarding rules that would automatically and
5 surreptitiously forward copies of incoming and/or outgoing emails
6 from certain employee email accounts to an email account controlled
7 by defendant OGUNGBESAN.

8 (d) SOUZA and BAKER would open bank accounts that could be
9 used to receive fraudulently obtained funds.

10 (e) SOUZA, BAKER, or other co-conspirators would provide
11 defendant OGUNGBESAN or other co-conspirators with account
12 information for the fraudulent bank accounts opened to receive
13 fraudulently obtained funds.

14 (f) In some instances, defendant OGUNGBESAN or a co-
15 conspirator would create fraudulent email accounts designed to trick
16 employees of a victim into believing that the accounts belonged to
17 businesses or individuals involved in the upcoming planned wire
18 transfers.

19 (g) In other instances, defendant OGUNGBESAN or a co-
20 conspirator would take control of genuine victim business email
21 accounts and communicate with BEC victim employees directly from
22 those accounts regarding upcoming planned wire transfers.

23 (h) Defendant OGUNGBESAN or a co-conspirator would
24 communicate with a victim - often fraudulently pretending to be a
25 company doing business with the victim - and would induce, or attempt
26 to induce, the victim to send a wire transfer to a fraudulent bank
27 account.

1 (i) SOUZA, BAKER, or other co-conspirators would withdraw
2 or transfer, or attempt to withdraw or transfer, the fraudulently
3 obtained funds from the bank account, and would further launder the
4 funds through transfers to additional bank accounts fraudulently
5 opened as part of the scheme so as to obtain the money and so as to
6 conceal and disguise the nature, location, source, ownership and
7 control of the proceeds.

8 C. OVERT ACTS

9 4. In furtherance of the conspiracy, and to accomplish its
10 objects, defendants OGUNGBESAN, SOUZA, and BAKER, together with
11 others known and unknown to the Grand Jury, on or about the dates set
12 forth below, committed and caused to be committed various overt acts,
13 in the Central District of California and elsewhere, including, but
14 not limited to, the following:

15 Overt Act No. 1: On an unknown date prior to June 1, 2019,
16 defendant OGUNGBESAN or a co-conspirator accessed email server(s)
17 used by Victim Business A, without authorization, and created an
18 unauthorized email forwarding rule causing copies of outgoing emails
19 from a Victim Business A employee account to be forwarded to an email
20 account controlled by OGUNGBESAN (the "OGUNGBESAN Email Account").

21 Overt Act No. 2: On January 16, 2019, defendant OGUNGBESAN or
22 a co-conspirator created a fraudulent email account appearing to be
23 victim K.S.'s true email address (the "False K.S. Email Address") and
24 registered the email account using victim K.S.'s name and date of
25 birth.

26 Overt Act No. 3: On January 16, 2019, defendant OGUNGBESAN or
27 a co-conspirator, using the False K.S. Email Address and posing as
28 victim K.S., sent an email attempting to redirect funds from a real

1 estate transaction involving Victim Business A to an account
2 controlled by OGUNGBESAN or a co-conspirator.

3 Overt Act No. 4: On April 1, 2019, defendant OGUNGBESAN or a
4 co-conspirator, without authorization, accessed email server(s) used
5 by Victim Business B, and instituted an unauthorized email forwarding
6 rule, causing copies of incoming and outgoing emails from a Victim
7 Business B employee email account to be forwarded to the OGUNGBESAN
8 Email Account.

9 Overt Act No. 5: On July 15, 2019, defendant OGUNGBESAN or a
10 co-conspirator, without authorization, accessed the email account of
11 Victim Business B's controller and used that account to send
12 fraudulent wiring instructions, causing approximately \$23,774,925 to
13 be wired to a bank account controlled by defendant OGUNGBESAN or a
14 co-conspirator.

15 Overt Act No. 6: In May 2019, defendant OGUNGBESAN or a co-
16 conspirator, without authorization, accessed email server(s) used by
17 Victim Business C, and instituted an unauthorized email forwarding
18 rule, causing copies of incoming and outgoing emails from a Victim
19 Business C employee email account to be forwarded to the OGUNGBESAN
20 Email Account.

21 Overt Act No. 7: On August 9, 2019, posing as an employee of
22 victim business Victim Business D, defendant OGUNGBESAN or a co-
23 conspirator sent an email with fraudulent wire instructions to an
24 employee of Victim Business C, causing approximately \$6,032,877
25 intended for Victim Business D to be wired to a bank account
26 controlled by defendant OGUNGBESAN or a co-conspirator.

27 Overt Act No. 8: On August 12, 2019, again posing as an
28 employee of Victim Business D, defendant OGUNGBESAN or a co-

1 conspirator sent an email with fraudulent wire instructions to an
2 employee of Victim Business C, causing Victim Business C to wire
3 approximately \$422,764 intended for Victim Business D to a bank
4 account controlled by defendant OGUNGBESAN or a co-conspirator.

5 Overt Act No. 9: On January 7, 2020, defendant OGUNGBESAN or
6 a co-conspirator, without authorization, accessed email server(s)
7 used by Victim Business E, compromised an existing Victim Business E
8 account with administrative privileges, and used that account to
9 create an unauthorized account with administrative privileges.

10 Overt Act No. 10: On January 11, 2020, defendant OGUNGBESAN,
11 without authorization, used the first unauthorized account with
12 administrative privileges to create a second unauthorized account
13 with administrative privileges, which was in turn used to conduct
14 searches to locate Victim Business E finance team email accounts.

15 Overt Act No. 11: On January 13, 2020, defendant OGUNGBESAN,
16 without authorization, accessed email used by Victim Business E, and
17 using the second unauthorized account with administrative privileges,
18 instituted an unauthorized email forwarding rule, causing copies of
19 incoming and outgoing emails from a Victim Business E employee email
20 account to be forwarded to the OGUNGBESAN Email Account.

21 Overt Act No. 12: On January 13, 2020, defendant OGUNGBESAN or
22 a co-conspirator conducted an online search for victim L.M.'s name,
23 employer, and business address.

24 Overt Act No. 13: On January 22, 2020, using the second
25 unauthorized account with administrative privileges, defendant
26 OGUNGBESAN or a co-conspirator began accessing Victim Business E
27 finance-team email accounts.

28 Overt Act No. 14: On February 15, 2020, defendant OGUNGBESAN

1 or a co-conspirator created a false email account appearing to belong
2 to Victim Business F ("False Victim Business F Email Address") and
3 registered the domain associated with the account using victim L.M.'s
4 name and victim L.M.'s credit card.

5 Overt Act No. 15: On February 15, 2020, defendant OGUNGBESAN
6 or a co-conspirator created a false email account appearing to belong
7 to Victim Business G ("False Victim Business G Email Address") and
8 registered the domain associated with the account using victim L.M.'s
9 name and victim L.M.'s credit card.

10 Overt Act No. 16: On February 18, 2020, using the False Victim
11 Business F Email Address and posing as an employee of Victim Business
12 F, defendant OGUNGBESAN or a co-conspirator sent an email to an
13 employee of Victim Business H regarding an upcoming scheduled wire
14 transfer.

15 Overt Act No. 17: On February 18, 2020, defendant OGUNGBESAN
16 or a co-conspirator, without authorization, accessed the email
17 account of Victim Business H's employee and, using that account,
18 emailed fraudulent wiring instructions to an employee of Victim
19 Business F, causing approximately \$3,100,000 to be wired to a bank
20 account controlled by OGUNGBESAN or a co-conspirator.

21 Overt Act No. 18: On February 20, 2020, defendant SOUZA sent
22 text messages to defendant BAKER stating, "We can get started
23 tomorrow" and "I'm going to send you something tonight I need you to
24 study The name of your company is [variation of Victim
25 Business G]."

26 Overt Act No. 19: On February 21, 2020, defendant SOUZA sent a
27 text message to defendant BAKER providing defendant BAKER with
28 fraudulent identity information to be used to open a bank account,

1 specifically, victim L.P.'s name with a misspelling of the last name,
2 victim L.P.'s date of birth, and victim L.P.'s social security
3 number, together with an email address.

4 Overt Act No. 20: On February 21, 2020, defendant SOUZA drove
5 defendant BAKER to a postal center in Douglasville, Georgia, where
6 defendant BAKER opened a P.O. Box using fraudulent identity
7 information provided by defendant SOUZA to be used as the mailing
8 address for Fraudulent Bank Account 1.

9 Overt Act No. 21: On February 21, 2020, defendant SOUZA and
10 defendant BAKER drove to a branch of Bank of America in Douglasville,
11 Georgia, where defendant BAKER opened Fraudulent Bank Account 1
12 purportedly for Fraudulent Business G, posing as the president of
13 Victim Business G and using a variation of victim L.P.'s name and
14 victim L.P.'s date of birth and social security number.

15 Overt Act No. 22: Between February 21, 2020, and February 26,
16 2020, defendant SOUZA or a co-conspirator provided the bank account
17 and wiring information for Fraudulent Bank Account 1 to defendant
18 OGUNGBESAN or a co-conspirator.

19 Overt Act No. 23: On February 25, 2020, defendant BAKER opened
20 Fraudulent Bank Account 2 using Fraudulent Business G as the account
21 name, posing as the president of Fraudulent Business G, and using a
22 variation of victim L.P.'s name and victim L.P.'s date of birth and
23 social security number.

24 Overt Act No. 24: On February 26, 2020, while accessing the
25 email account of Victim Business E employee J.B. without
26 authorization and posing as J.B., defendant OGUNGBESAN or a co-
27 conspirator sent an email to a Victim Business E employee intending
28 to provide the wiring information for Fraudulent Bank Account 1 but

1 including a typographical error in the bank account number.

2 Overt Act No. 25: On February 28, 2020, defendant SOUZA sent a
3 text message to defendant BAKER regarding a 1.6 million dollar
4 payment and stating, "GOD willing it goes through."

5 Overt Act No. 26: On February 28, 2020, defendant SOUZA sent a
6 text message to defendant BAKER stating, "You taking 20% of 1.6."

7 Overt Act No. 27: On March 30, 2020, while accessing the email
8 account of Victim Business E employee J.B. without authorization and
9 posing as J.B., defendant OGUNGBESAN or a co-conspirator sent an
10 email to Victim Business E employee D.R. containing purportedly
11 corrected wiring information for Fraudulent Bank Account 1, but
12 including a typographical error in the routing number.

13 Overt Act No. 28: On April 23, 2020, defendant OGUNGBESAN or a
14 co-conspirator, posing as Victim Business G employee, sent an email
15 with the correct routing information for Fraudulent Bank Account 1,
16 which caused Victim Business E to wire a payment intended for Victim
17 Business G of \$1,746,505 to Fraudulent Bank Account 1.

18 Overt Act No. 29: On April 24, 2020, defendants SOUZA and
19 BAKER went to a Bank of America branch in Stockbridge, Georgia, where
20 defendant BAKER withdrew \$9,200 in cash from Fraudulent Bank Account
21 1.

22 Overt Act No. 30: On April 24, 2020, while at the Bank of
23 America branch in Stockbridge, Georgia, defendant BAKER withdrew
24 \$300,000 from Fraudulent Bank Account 1 in the form of a cashier's
25 check made payable to Fraudulent Business G.

26 Overt Act No. 31: On April 25, 2020, defendants SOUZA and
27 BAKER went to a Bank of America branch in Savannah, Georgia, where
28 defendant BAKER withdrew \$9,300 cash from Fraudulent Bank Account 1

1 and unsuccessfully attempted to send a larger wire transfer of funds
2 from Fraudulent Bank Account 1.

3 Overt Act No. 32: On April 25, 2020, defendants SOUZA and
4 BAKER went to a different Bank of America branch in Savannah,
5 Georgia, where defendant BAKER unsuccessfully attempted to send a
6 \$500,000 wire transfer from Fraudulent Bank Account 1.

7 Overt Act No. 33: On April 27, 2020, defendant BAKER opened
8 Fraudulent Bank Account 3 at BB&T Bank in Morrow, Georgia, using
9 Fraudulent Business G as the account name, posing as the president of
10 Fraudulent Business G, with incorporation documents for Fraudulent
11 Business G, and using a variation of victim L.P.'s name and victim
12 L.P.'s date of birth and social security number.

13 Overt Act No. 34: On April 27, 2020, defendant BAKER deposited
14 the \$300,000 cashier's check issued by Bank of America into
15 Fraudulent Bank Account 3.

16 Overt Act No. 35: On April 27, 2020, OGUNGBESAN or a co-
17 conspirator sent fraudulent wiring instructions to Victim Business G,
18 causing Victim Business G to wire approximately \$958,664 to
19 Fraudulent Bank Account 1.

COUNT TWO

[18 U.S.C. § 1028A(a) (1); 2(b)]

[DEFENDANT KOLAWOLE TEMIDAYO OGUNGBESAN]

Beginning on an unknown date, but no later than on or about January 15, 2019, and continuing through at least April 27, 2020, in Riverside County, within the Central District of California, and elsewhere, defendant KOLAWOLE TEMIDAYO OGUNGBESAN, also known as ("aka") "Engr Jah," aka "Rich Jah," aka "Kolawole Churchill," aka "Bombo Klaat" ("OGUNGBESAN"), knowingly transferred, possessed, and used, and willfully caused to be transferred, possessed, and used, without lawful authority, a means of identification that defendant OGUNGBESAN knew belonged to another person, during and in relation to the offense of conspiracy to commit wire fraud and bank fraud, a felony violation of Title 18, United States Code, Section 1349, as charged in Count One of this Indictment.

COUNT THREE

[18 U.S.C. §§ 1343; 2(a)]

[DEFENDANT KOLAWOLE TEMIDAYO OGUNGBESAN]

1. The Grand Jury re-alleges and incorporates here paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment.

A. THE SCHEME TO DEFRAUD

2. Beginning on an unknown date, but no later than on or about January 15, 2019, and continuing through at least April 27, 2020, in Los Angeles, Orange, and San Bernardino Counties, within the Central District of California, and elsewhere, defendant KOLAWOLE TEMIDAYO OGUNGBESAN, also known as ("aka") "Engr Jah," aka "Rich Jah," aka "Kolawole Churchill," aka "Bombo Klaat" ("OGUNGBESAN"), together with others known and unknown to the Grand Jury, each aiding and abetting the other, knowingly and with intent to defraud, devised, participated in, executed and attempted to execute a scheme to defraud a victim as to material matters, and to obtain money and property from such victim by means of material false and fraudulent pretenses, representations, and promises, and the concealment of material facts.

3. The fraudulent scheme to defraud operated and was carried out, in substance, as set forth in the manner and through the means described in Section B. of Count One of this Indictment, which is incorporated as if fully set forth herein.

B. USE OF THE WIRES

4. On or about January 16, 2019, at approximately 8:07 a.m. PST, in Orange and San Bernardino Counties, within the Central District of California and elsewhere, for the purpose of executing

1 the above-described scheme to defraud, defendant OGUNGBESAN
2 transmitted and caused others to transmit, by means of wire
3 communication in interstate and foreign commerce, an email from a
4 fraudulent email account appearing to belong to victim K.S. to an
5 individual working on a real estate transaction involving Victim
6 Business A in the Central District of California.

COUNT FOUR

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I); 2(a)]

[DEFENDANT KOLAWOLE TEMIDAYO OGUNGBESAN]

1. The Grand Jury re-alleges and incorporates here paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment.

2. On or about January 13, 2020, in Orange County, within the Central District of California, and elsewhere, defendant KOLAWOLE TEMIDAYO OGUNGBESAN, also known as ("aka") "Engr Jah," aka "Rich Jah," aka "Kolawole Churchill," aka "Bombo Klaat" ("OGUNGBESAN"), together with others known and unknown to the Grand Jury, each aiding and abetting the other, knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems, and information on a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), namely, the email server(s) used by Victim Business E, thereby causing a loss aggregating at least \$5,000 in value during a one-year period beginning on January 13, 2020, to Victim Business E.

COUNT FIVE

[18 U.S.C. § 1956(h)]

[ALL DEFENDANTS]

1. The Grand Jury re-alleges and incorporates here paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECT OF THE CONSPIRACY

2. Beginning on an unknown date, but no later than on or about January 15, 2019, and continuing through at least April 27, 2020, in Los Angeles, Orange, and San Bernardino Counties, within the Central District of California, and elsewhere, defendants KOLAWOLE TEMIDAYO OGUNGBESAN, also known as ("aka") "Engr Jah," aka "Rich Jah," aka "Kolawole Churchill," aka "Bombo Klaat" ("OGUNGBESAN"), SHOLA SOUZA ("SOUZA"), and DEON BAKER ("BAKER"), together with others known and unknown to the Grand Jury, knowingly conspired to conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, which, in fact, involved the proceeds of specified unlawful activity - namely, Wire Fraud, in violation of Title 18, United States Code, Section 1343 - and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

B. THE MANNER AND MEANS OF THE CONSPIRACY

3. The object of the conspiracy was to be accomplished, in substance, as follows:

(a) Defendant OGUNGBESAN or a co-conspirator would cause a

1 bank account to be opened into which defendant OGUNGBESAN or a co-
2 conspirator could fraudulently induce a victim to deposit funds from
3 a BEC fraud or other fraudulent scheme.

4 (b) Defendant SOUZA, defendant BAKER, or other co-
5 conspirators would send account information to defendant OGUNGBESAN
6 or others acting at his direction for bank accounts that could be
7 used to receive fraudulently obtained funds.

8 (c) Defendant OGUNGBESAN or a co-conspirator would,
9 through false or fraudulent pretenses, representations, and promises,
10 and concealment of material facts, cause a victim to deposit, wire,
11 or transfer funds into the bank accounts opened by defendants SOUZA
12 and BAKER, and/or other co-conspirators.

13 (d) Defendant BAKER, acting at the direction of defendant
14 SOUZA, would withdraw or attempt to withdraw the fraudulently
15 obtained funds from the bank account, including through cash
16 withdrawals, wire transfers, issuance of cashier's checks, and
17 deposits into further accounts used by co-conspirators, before the
18 victim became aware of the fraudulent nature of the transactions, so
19 as to obtain the money and so as to conceal and disguise the nature,
20 location, source, ownership and control of the proceeds.

21 C. OVERT ACTS

22 4. In furtherance of the conspiracy, and to accomplish its
23 objects, defendants OGUNGBESAN, SOUZA, and BAKER, together with
24 others known and unknown to the Grand Jury, on or about the dates set
25 forth below, committed and caused to be committed various overt acts
26 in the Central District of California, and elsewhere, including, but
27 not limited to, the following:

28 Overt Act Nos. 1-24: The Grand Jury re-alleges and

incorporates here Overt Act Numbers 9, 10, 11, 12, 13, 15, and 18-35
of Section C of Count One of this Indictment.

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 982]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(1) and (2), in the event of any defendant's conviction of the offenses set forth in any of Counts One, Two, or Five of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense; and

(b) Any Property, real or personal, involved in such offense, and any property traceable to such property;

(c) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been

1 substantially diminished in value; or (e) has been commingled with
2 other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of the defendant's conviction of the offense set forth in Count Three of this Indictment.

2. The defendant, if so convicted, shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), the defendant, if so convicted, shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of the defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION THREE

[18 U.S.C. §§ 982 and 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1030, in the event of defendant's conviction of the offense set forth in Count Four of this Indictment.

2. The defendant, if so convicted, shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

(b) Any property used or intended to be used to commit the offense; and

(c) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

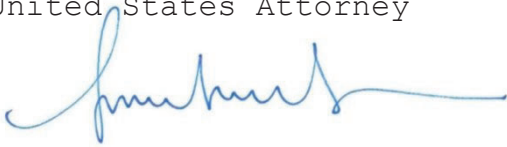
Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i), defendant, if so convicted, shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has

1 been commingled with other property that cannot be divided without
2 difficulty.

3
4 A TRUE BILL

5
6 /s/
7 Foreperson

8 E. MARTIN ESTRADA
9 United States Attorney

10 

11 ANNAMARTINE SALICK
12 Assistant United States Attorney
13 Chief, National Security Division

14 CAMERON L. SCHROEDER
15 Assistant United States Attorney
16 Chief, Cyber & Intellectual
17 Property Crimes Section

18 LISA E. FELDMAN
19 Assistant United States Attorney
20 Cyber & Intellectual Property
21 Crimes Section

22 AARON FRUMKIN
23 Assistant United States Attorney
24 Cyber & Intellectual Property
25 Crimes Section
26
27
28